REMARKS

Status of the Claims

Prior to entry of this paper, Claims 1-33 were pending. Claims 1-33 were rejected. In this paper, no claims are amended, cancelled or added. Upon entry of this paper, Claims 1-33 will be currently pending. For at least the following reasons, Applicant respectfully submits that each of the presently pending claims is in condition for allowance.

Claim Rejections – 35 U.S.C. § 103(a)

Claim 32 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright et al., U.S. Patent No. 7,308,703 B2 (hereinafter "Wright") and further in view of Knouse et al., U.S. Patent No.. 7,185,364 B2 (hereinafter "Knouse"). Claims 1-2, 4-11, 13-18 and 20-31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright and further in view of Shah et al., U.S. Patent No. 7,430,524 B2 (hereinafter "Shah") and Knouse. Claim 19 was rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Wright, Knouse, and Shah, as applied to Claim 10 above and further in view of Ishikawa, U.S. Patent No. 7,200,272 B2 (hereinafter "Ishikawa"). Claims 3 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Wright, Knouse, and Shah, and further in view of Levine, U.S. Patent Application Publication No. 2002/0111852 A1 (hereinafter "Levine"). Claim 33 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright and further in view of Levine and Knouse.

Claim 1 recites, in part:

> *receiving from the downloaded component the configuration of the client device based on the inspection;*
> *in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the received configuration and the requested resource*

In contrast, Wright discusses a mobile device enforcing a security policy on the same mobile device based on the location of the mobile device and security features detected on the mobile device.[1] In other words, Wright discusses a device applying a security policy to itself based on properties of itself. For example, Wright chooses a security policy based the type of network connection the mobile device is using, whether the mobile device's NIC has enhanced security features such as 802.11i, and the presence or absence of security software such as VPN software and anti-virus software.[2] Each of these security features is a property of the mobile device itself, not of a different device. Thus, none of these security features teach or even suggest a configuration of a different device. Therefore, Wright's selection of security policy fails to teach or suggest "receiving from the downloaded component the configuration of the client device based on the inspection; [and] in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the received configuration and the requested resource" as recited in Claim 1.

Examples of security policies discussed by Wright include hiding or encrypting files on the mobile device[3] as well as filtering incoming and outgoing network traffic to the mobile device.[4] While it is true that dropping packets sent from another device does nominally mention another device, these packets are not dropped based on a received configuration of the other device. Instead, Wright discusses dropping these packets based on the destination port of the packet (for example, if a port associated with file sharing), the MAC address of the mobile device's network access point, the source IP address, etc.[5] Clearly, none of these parameters teaches or suggests a configuration of the device sending the packets, and so dropping a packet based on these properties does not teach applying a dynamic policy based on a received configuration of another device. Therefore, Wright's selectively dropping of packets also fails to teach or suggest "receiving from the downloaded component the configuration of the client device based on the inspection; [and] in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the received configuration and the requested resource" as recited in Claim 1.

[1] *See* Wright, abstract.
[2] *See* Wright 7:14-37.
[3] *See* Wright 2:49-53.
[4] *See* Wright 7:51-67.
[5] *See* Wright 15:20-67.

Knouse fails to cure the deficiencies of Wright. While it is true that Knouse discusses a server receiving a request for a resource, authenticating the user requesting the resource, and authorizing access to the resource based on a directory server 36 associated with the server, none of these features teach or suggest applying a policy based on a received configuration. Clearly, the received request is not a configuration of the requesting device. Also, the received login information is clearly not a configuration of the requesting device.

Moreover, even a combination of Wright and Knouse fails to teach or suggest these elements. Both Wright and Knouse discuss receiving requests for resources (Wright for files,[6] and Knouse for resources generally[7]), Wright filtering packets based on destination port, MAC address of a network access point, etc., and Knouse filtering requests based on a user's authentication and authorization. Thus, even a combination of Wright and Knouse fails to teach or suggest applying a dynamic policy for access based on a received configuration of the requesting client device, as recited. Therefore, even the proposed combination of Wright and Knouse fails to teach or suggest "receiving from the downloaded component the configuration of the client device based on the inspection; [and] in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the received configuration and the requested resource" as recited in Claim 1.

Independent Claims 10, 22, 28, 31, and 32 recite elements that are similar to, yet different from, the elements recited in amended Claim 1. Accordingly, independent Claims 10, 22, 28, 31, and 32 are allowable for at least the same reasons as discussed above with regard to Claim 1. Shah fails to cure the deficiencies of Wright and Knouse. In contrast, Shah discusses downloading a program to a client and determining information regarding a plurality of devices and programs on the client.[8] While Shah discusses using this information for documenting and modifying the client system configuration, as well as adding/removing programs or devices to/from the client system,[9]

[6] *See* Wright 15:55-67.

[7] *See* Knouse 8:32-67.

[8] *See* Shah, column 76 lines 9-15.

[9] *See* Shah, column 77 lines 55-57.

Shah does not teach or even suggest the recited apparatus applying a restriction to the client device. Therefore, even the proposed combination of Wright, Knouse, and Shah fails to teach or suggest "in response to the received request, applying, using the server device, a dynamic policy to the access based, in part, on the determined level of security software enabled and the requested resource" as recited in Claim 1.

Furthermore, since dependent Claims 2-9, 11-21, 23-27, and 29-30 are at least allowable for the same reasons as independent Claims 1, 10, 22, and 28 upon which they depend respectively, the rejection of these claims is now moot. Accordingly, Applicants' representative respectfully requests the rejection under 35 U.S.C. §103(a) of Claims 1-33 be withdrawn.

Amended dependent Claim 9 is allowable for additional reasons. Dependent Claim 9 recites "*wherein applying the restriction further comprises performing at least one of inhibiting a file save and inhibiting a file print*". In making out the rejection of Claim 9, the Office Action cites Wright column 20 lines 35-42, which discusses preventing a hacker from co-opting the user's device and coming in to the corporate network. The Office Action asserts that preventing a hacker from accessing the network would inhibit a file save by preventing write access to hackers. Applicants' representative respectfully disagrees, and instead points out that preventing a file save as recited is applying a restriction to the client device for access to the requested resource (see Claim 1). Clearly, keeping a hacker out of a corporate network has nothing to do with restricting access to a requested resource. For this additional reason, even the proposed combination of Wright, Shah, and Knouse fails to teach or suggest "wherein applying the restriction further comprises performing at least one of inhibiting a file save and inhibiting a file print" as recited in Claim 9.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-33) are now in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicant's representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicant reserves the right to raise these arguments in the future.

Dated: January 13, 2011

Respectfully submitted,

By /David W. Foster/
David W. Foster
Registration No.: 60,902
FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, NY 10151
(206) 336-5672
(212) 588-0500 (fax)
Attorneys/Agents For Applicant